



US Army Reserve Information Operations



The United States Army Reserve Information Operations Structure (ARIOS)

POCs: COL Ed Magdziak/MAJ Jet Bibler
CIO/Force Programs
Office of the Chief, Army Reserve
Work: 703-602-3055/703-601-3472

28 October 2002



Information Operations



Actions taken to affect adversary information and information systems while defending one's own information and information systems (JP 3-13).

Changes to Five Elements (OPSEC, EW, Deception, PYSOP and CNO) with release of new DODD 3600.1

Elements

OPSEC	Physical Destruction	Information Assurance	Counter-PSYOP
Military Deception	Computer Network Attack	Physical Security	Counter-Intel
PSYOP	Special IO	Counter-deception	Public Affairs
EW			Civil Affairs

Offensive IO

Employ IO elements to affect and/or influence leader perceptions/decisions.

- Inform, influence or deceive leaders.
- Deny, disrupt, destroy or control adversary info, info systems & C4ISR.
- Exploit timely, precise information and/or attack targets.

Defensive IO

Employ IO elements to protect friendly info, info systems and C4ISR:

- Protect, detect, restore and respond .
- Manage risk and deter attacks.
- Protect C2 process, info, personnel, facilities and equipment.
- Influence leader perceptions/decisions.



Army Reserve Support to Information Superiority



**INFORMATION
MANAGEMENT**

**INFORMATION
OPERATIONS**

**RELEVANT
INFORMATION**

INFOSYS

**DEFENSIVE
IO**

**OFFENSIVE
IO**

**Military Intelligence
Production
Groups/Detachments**

**Army Reserve
Information
Command (ARIOC)**

**Enhancement
Center (IWECC)**

**Existing PSYOP
Public Affairs
Military Intelligence
Other Operational
Skills**

Civilian Acquired Skills Database (CASDB)



Who is driving IO in Joint Community?



Other Players

OSD

Joint Reserve Virtual
Information
Operations (JRVIO)
Organizations

DISA

LTG Raduege (USAF)



IO Combatant Command

USSTRATCOM
ADM Ellis (USN)
Effective 1 Oct 02



CDR JTF-CNO
MG Bryan (USA)
Vice Director, DISA
Effective 1 April 01



JIOC
MG Wright (USAF)



Other Players

NSA
LTG Hayden (USAF)
(IOTC/JCMA)

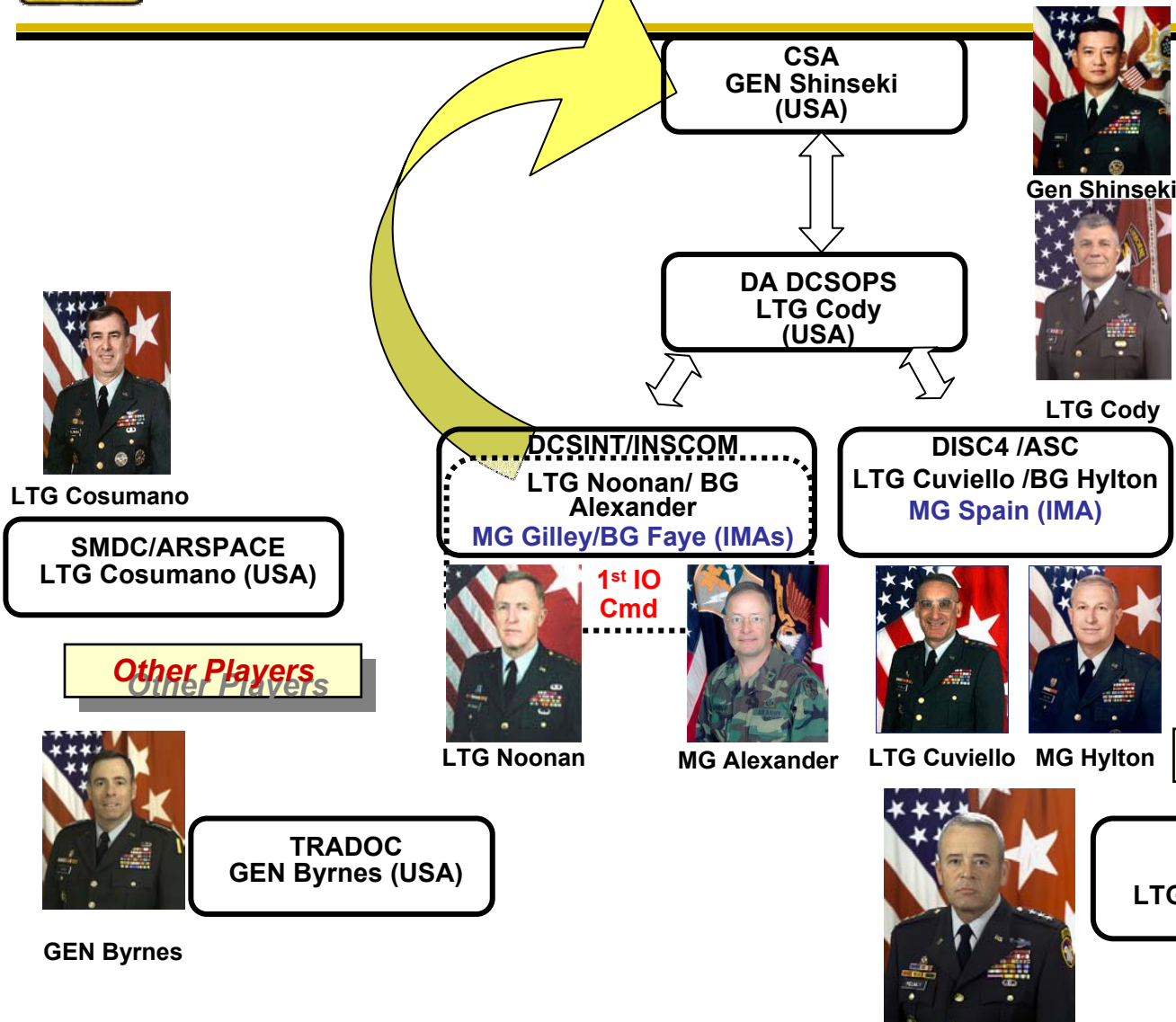


Information Operations is D.C. Centric:

- Fragment C2
- Combatant Commander working towards clear direction
- Subset of Home Land Defense/Consequence Management
- Congressional view of IO is Critical Information Infrastructure Protection

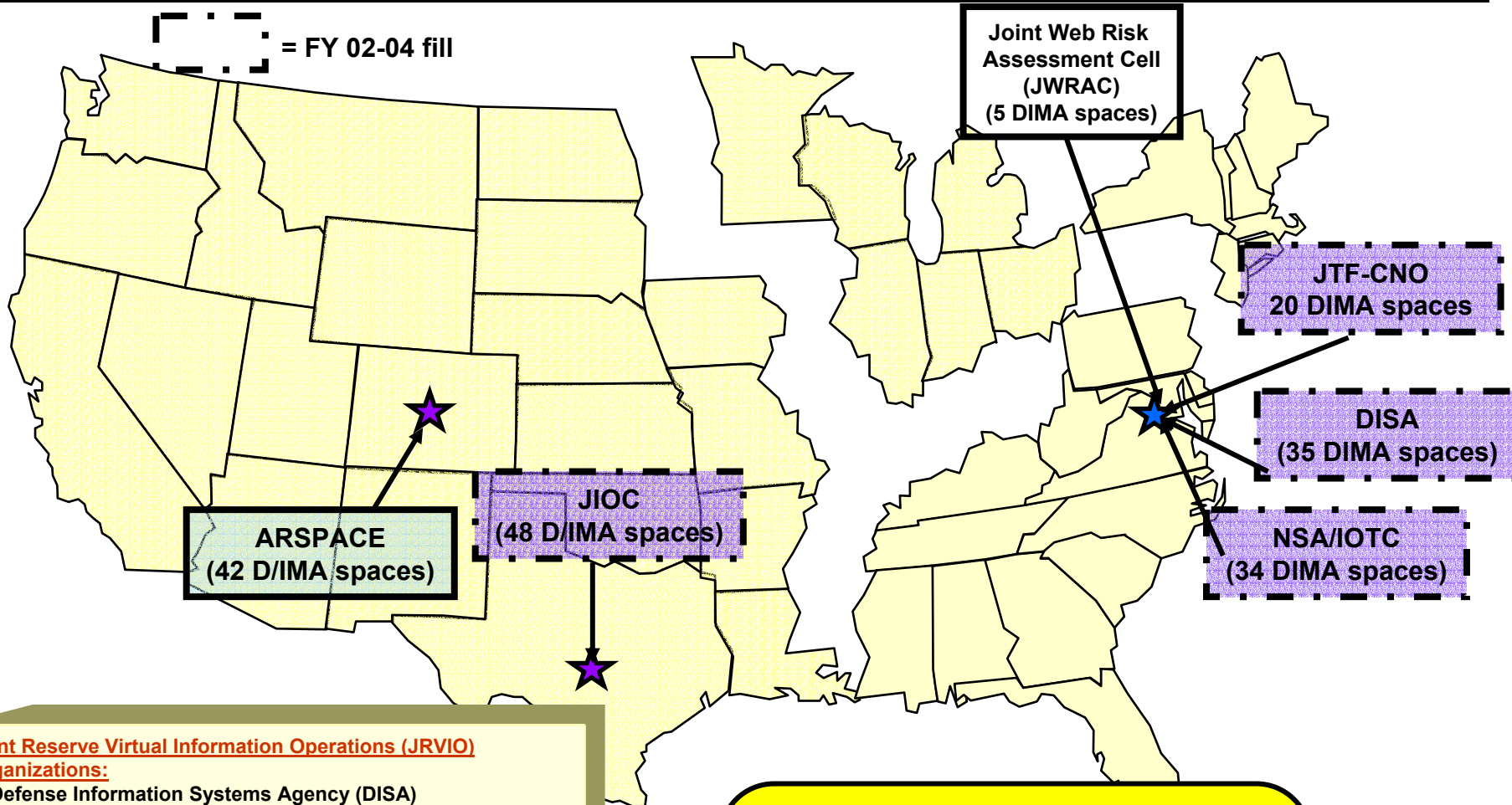


Who is driving IO in Army?





Army Reserve Contributory Support in IO



Joint Reserve Virtual Information Operations (JRPIO)

Organizations:

- ✓ Defense Information Systems Agency (DISA)
- ✓ JTF-Computer Network Defense (CNO/DISA)
- ✓ Information Operations Technology Center (IOTC/NSA)
- ✓ Joint COMSEC Monitoring Activity (JCMA/NSA)
- ✓ Joint Information Operations Center (JIOC/USSPACECOM)

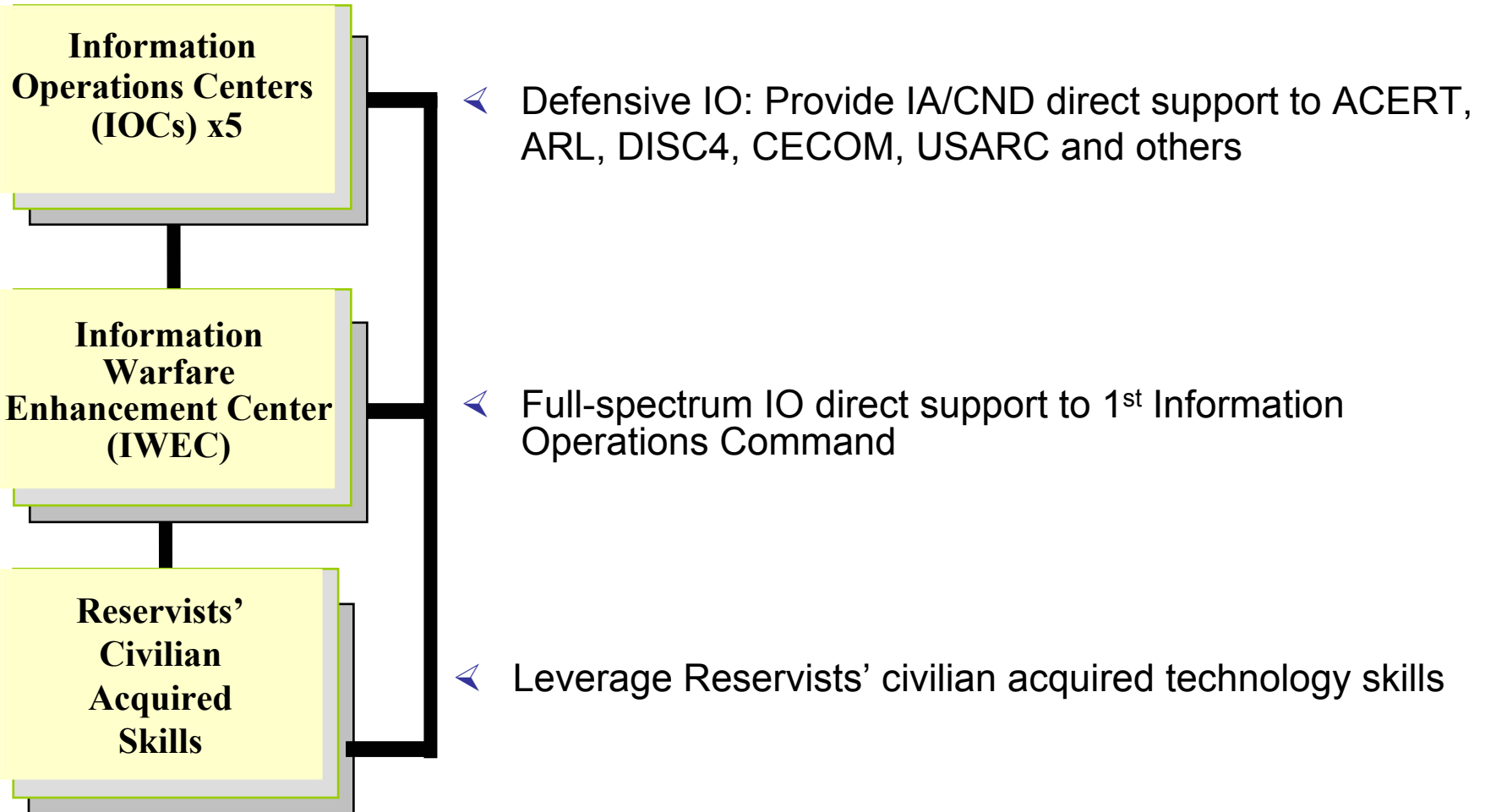
184 Authorizations



US Army Reserve Information Operations Command Structure

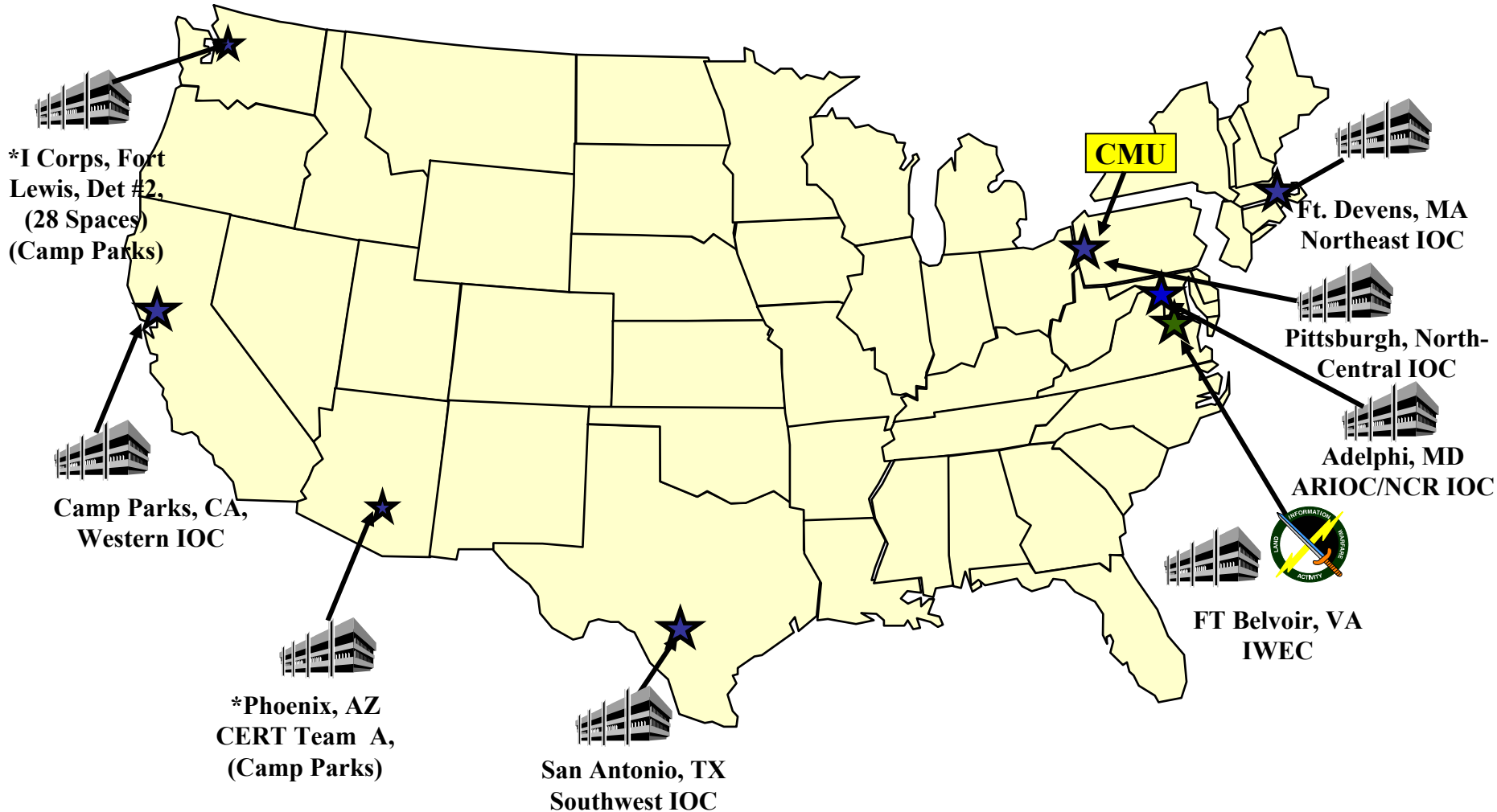


IO Capability





Army Reserve Information Operations Locations



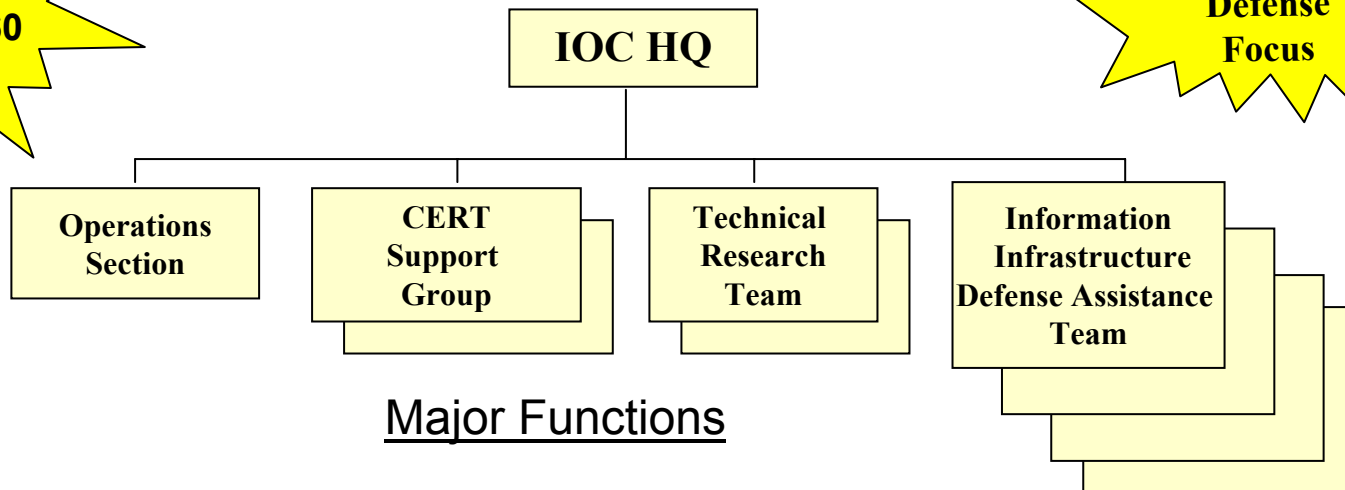


Information Operations Center (IOC)



90 Spaces
(Authorized 60 spaces)

Computer Network Defense Focus



- Information Assurance
- Viral Detection and Protection
- Vulnerability Assessment
- Intrusion Detection & Response

- Incident Analysis
- Vulnerability Database
- High Performance Computer Monitoring



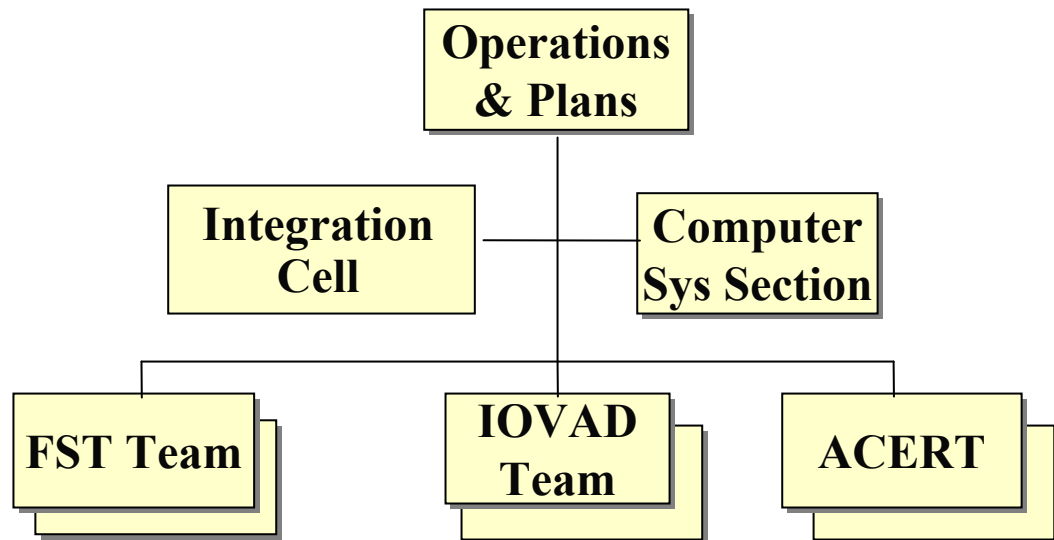
Information Warfare Enhancement Center (IWECC)



Missions & Functions integrated with 1st Information Operations Command (17 Oct 02):

- Field Support
- Vulnerability Assessment
- Viral Detection and Protection
- Vulnerability Intrusion Detection & Response
- Information Assurance

**73 Total
Spaces**



**Part of 1st IO Cmd
Multi-Compo Organization**



ARIOS IA Capability



Protect, Detect & Assess Restore, Respond

- Enhance DOD Computer Network Defense
 - Viral Detection and Protection
 - Intrusion Detection and Protection
 - Predictive Analysis
 - Vulnerability Analysis and Assessments
 - Document Advisories
 - Training and Education
- Help DOD Transition Corporate Improvements
 - Civilian Acquired Skills



Army Reserve IO Mission FY 2000-2002



Technical Missions

- Joint Staff (J8) Network Scans
- Army Computer Emergency Response Team (ACERT) Monitoring

Army Research Lab (ARL)
Computer Intrusion Monitoring
Program

JTF-CNO Support

CECOM Survivability Lethality
Analysis Directorate (SLAD)
Vulnerability Assessment and
Database Support

Vulnerability
Assessment Teams
(VAT) in Balkans

Joint Reserve Virtual Information Operations (JRVIO) Organizations

Operational Missions

- Field Support to Corps and Joint Exercises
- Individual IO Support to Army and Joint Commands

CORPS Warfighter Exercise
Support

DISC4 Information Assurance
Vulnerability Assessment (IAVA)
Compliance

**Army Reserve IO Support primarily at
Corps, Theater, DA, and Joint level**



ARIOS Soldier Skills



- Corporate IT Executives
- Microsoft Certified Systems Engineers (MCSE)
- Defense Messaging System (DMS) Specialists
- Corporate Software Developers
- Computer Network Defense Experts
- Corporate and Government Computer Security Professionals
- System/Network Administrators
- Soldiers with advanced Computer Science Degrees

Reduces Army's Critical IA Skill Shortfalls



Summary



- *The Army Reserve* supports Information Superiority:
- Full-spectrum offensive and defensive IO
- IO units, augmentation, and skilled soldiers
- Enhances Army organizations with flexible capabilities
- Leverages USAR Information Operations core competencies
- Capitalizes on citizen-soldiers' high-technology civilian skills
- Expanding and developing new capabilities

Army Reserve Supports Information Operations



Back-up Slides





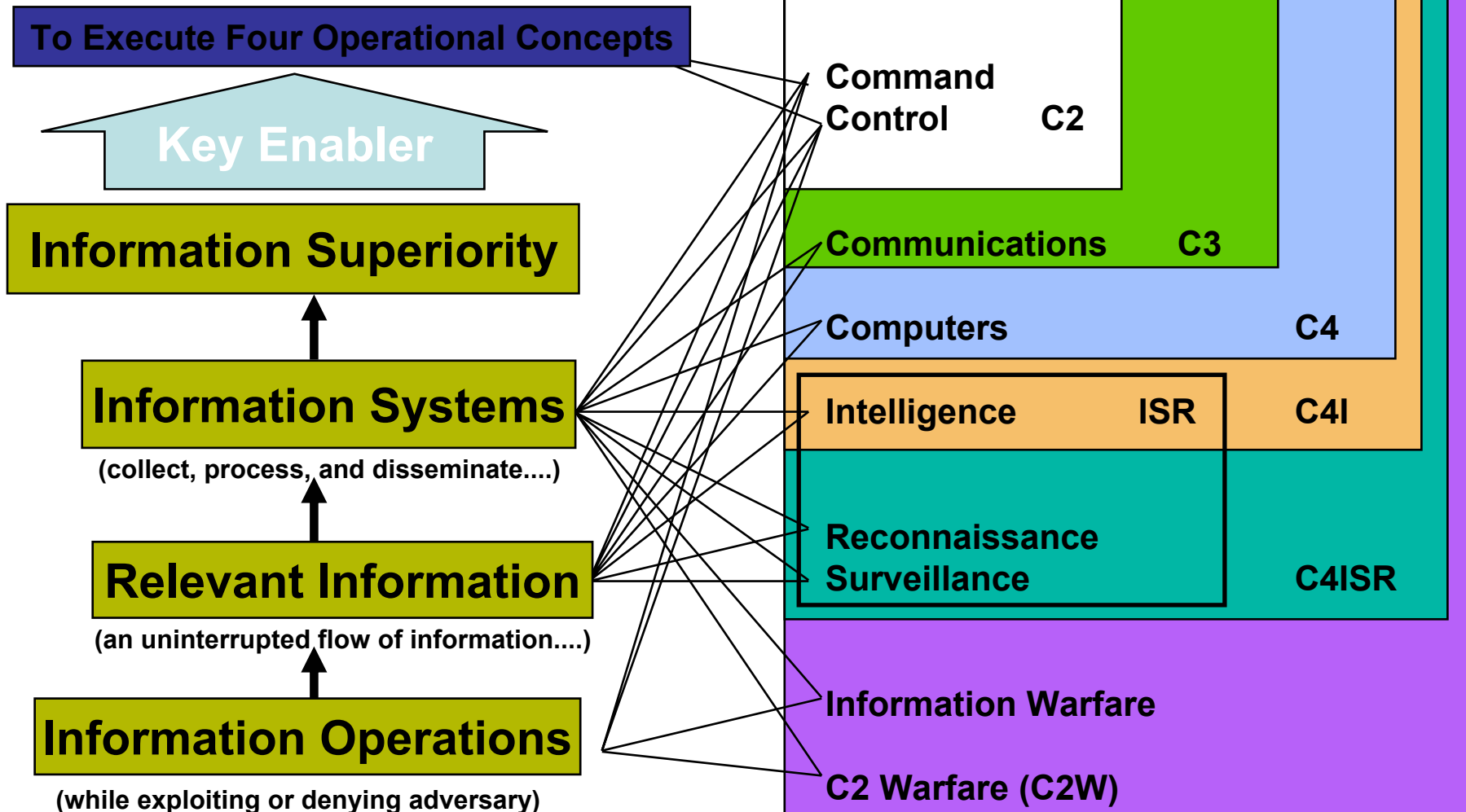
Information Operations



Information Superiority: JV 2010 Construct

JV 2010 Construct

Other Terms





Information Operations Definitions (U)



Information Operations - *DoD Directive S-3600.1*

(U) Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Warfare - *DoD Directive S-3600.1*

(U) Information Operations conducted during time of crisis or conflict to achieve specific objectives over a specific adversary or adversaries.

Information Operations - *JP 3-13*

(U) Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Command & Control Warfare - *JP 3-13.1*

As a subset of IW, command and control warfare (C2W) is an application of IW in military operations that specifically attacks and defends the command and control (C2) target set.



Information Operations (IO) Program



Definitions

➤ **Information Operations (IO):** Actions taken to influence, affect or defend information, information systems and decision-making. Draft DOD Directive S-3600.1 Version 6.1

➤ **Information Operations (IO):** Actions taken to affect an adversary's information and information systems while defending one's own information and information systems JP1-02 and JP 3-13

➤ **Army's Definition of Information Operations (IO):** Information operations are actions taken to affect adversary, and influence others', decision making processes, information and information systems while protecting one's own information and information systems. FM 3-0 14 Jun 2001

➤ **Army Elements of Information Operations (IO):** Military deception, Counterdeception, Operations security, Physical security, Electronic warfare, Electronic attack, Electronic protection, Electronic warfare support, Information assurance, Physical destruction, Psychological operations, Counterpropaganda, Counterintelligence, Computer network attack, Computer network defense. FM 3-0, 14 Jun 2001

➤ **Joint Reserve Virtual Information Operations (JRVIO) Organizations:**

- ✓ Defense Information Systems Agency (DISA)
- ✓ JTF-Computer Network Defense (CNO/DISA)
- ✓ Information Operations Technology Center (IOTC/NSA)
- ✓ Joint COMSEC Monitoring Activity (JCMA/NSA)
- ✓ Joint Information Operations Center (JIOC/USSPACECOM)

➤ **Computer Network Defense (CND):** Computer network defense consists of all measures to defend computers and other components that are interconnected in electronic telecommunications networks against computer network attacks by an adversary. Such measures include access controls, detection of malicious computer code and programs, and tools to detect intrusions. Army forces use inherent capabilities and accomplish specific computer network defense actions to defend computer networks from unauthorized users. FM 3-0, 14 Jun 2001

➤ **Computer Network Attack (CNA):** Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Draft DOD Directive S-3600.1 Version 6.1

➤ **Information Assurance (IA):** Actions to protect and defend information and information systems which ensures the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems. Note: IA incorporates protection, detection, reaction, and restoration capabilities within information systems. Computer network defense (CND) is an operational component of IA and a core capability of IO that provides guidance in response to specific threats. Draft DOD Directive S-3600.1 version 6.1



Information Operations DoD IO Policy & Goal



- ***Policy:** (U) DoD activities shall be organized, trained, equipped, and supported to plan and execute IO - DoD Directive S-3600.1*
- ***Goal:** (U) IO is to secure peacetime national security objectives, deter conflict, protect DoD information systems, and to shape the information environment - DoD Directive S-3600.1*
- ***Goal of IO is to insure we don't do IW***



Information Operations

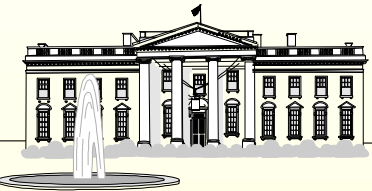
Potential IO Targets That May Influence the KEY Decision Maker(s)



Examples of IW Targets

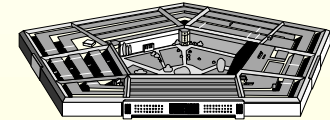
Leadership

- Key Personnel
- ADP Support
- Strategic Comms
- Power Base



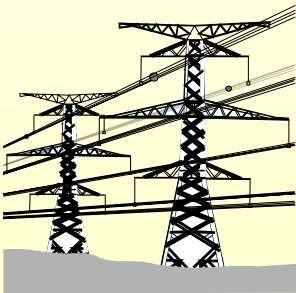
Military Infrastructure

- Commanders
- C2 Comm Links
- C2 Nodes
- Troops
- Intel Collectors



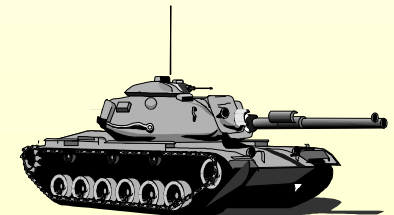
Civil Infrastructure

- Comms (Links/Nodes)
- Industry
- Financial
- Populace



Weapons Systems

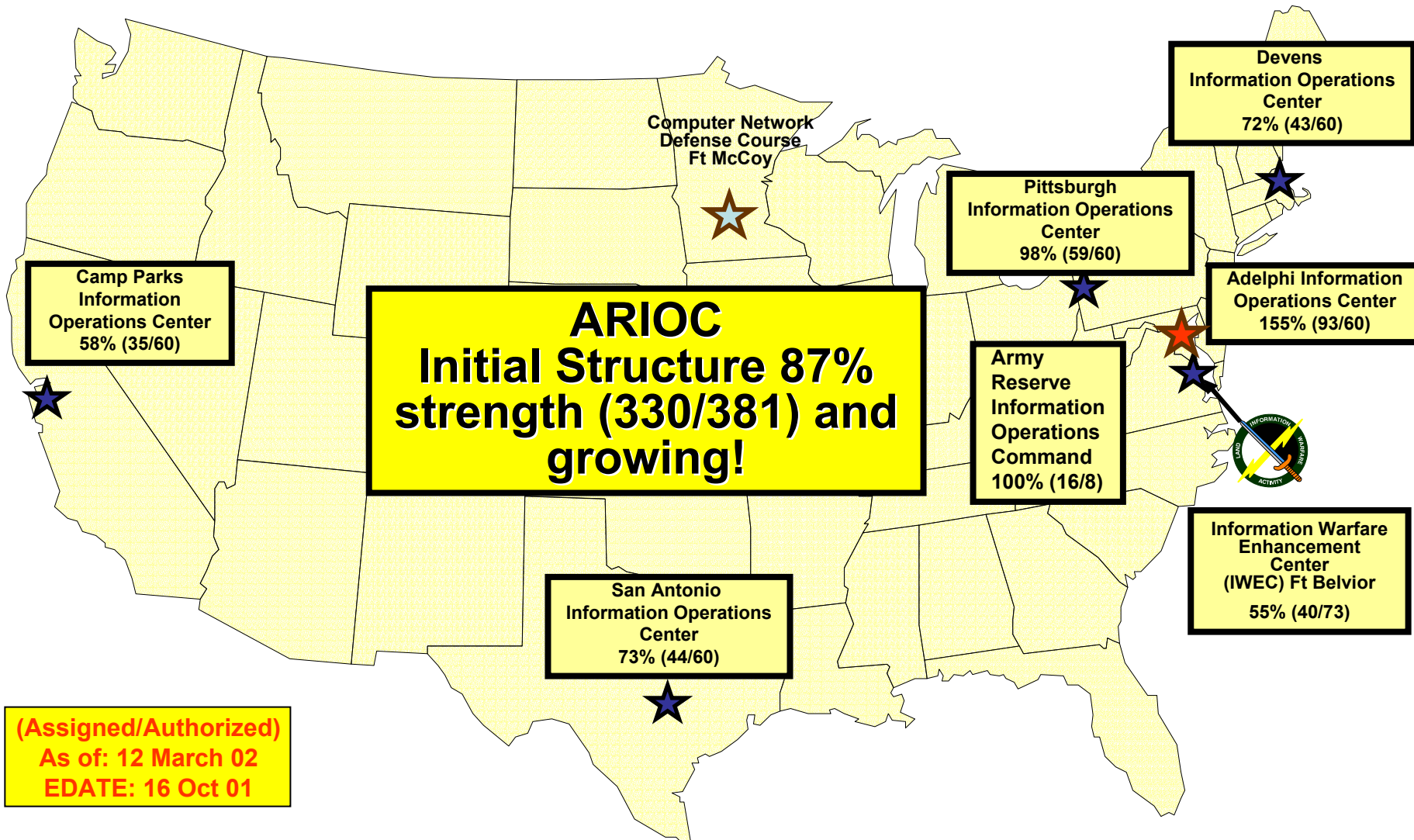
- Planes
- Ships
- Artillery
- PGMs
- Air Defense





A Successful Beginning....

... that Prepares us for Future Growth





Current Command Relationships Roles

